DISA JIEO Standards Analysis **15 FEB 00**

RFC 2634 Enhanced Security Services for S/MIME

References:

```
RFC 2634, Enhanced Security Services for S/MIME
RFC 2630, Cryptographic Message Syntax
RFC 2632, S/MIME Version 3 Certificate Handling
```

Implementation under analysis:

Analysis Date:

REQUIREMENT FROM STANDARDS [1]	MET (Y/N/ na)	NOTES
Is triple wrapping used when a message must be signed, then encrypted, and then have signed attributes bound to the encrypted body? [RFC 2634 1.1.1]		
In the triple wrapping process, when an inner MIME header and the original content are signed is the SignedData encapContentInfo eContentType object identifier id-data? [RFC 2634 1.1.2(3)]		
In the triple wrapping process, if the inside signature structure is multipart/signed, is SignedData encapContentInfo eContent absent? [RFC 2634 1.1.2(3)]		
In the triple wrapping process, if the inside signature structure is application/pkcs7-mime, then does the SignedData encapContentInfo eContent contain the original content with the appropriate MIME content-type header? [RFC 2634 1.1.2(3)]		
In the triple wrapping process, is the EnvelopedData encryptedContentInfo contentType id-data? [RFC 2634 1.1.2(5)]		
Is the receiving agent able to interpret either multipart/signed or application/pkcs7-mime signature structures? [RFC 2634 1.2]		
If the message is triple wrapped with a signed receipt request, is the receipt request in the inside signature? [RFC 2634 1.3.1]		
Is an eSSSecurityLabel attribute only used in a signedAttributes block and not used in an EnvelopedData or unsigned attribute? [RFC 2634 1.3.2]		

REQUIREMENT FROM STANDARDS [1]	MET (Y/N/ na)	NOTES
If the attributes contentReference, equivalentLabel, eSSSecurityLabel and mlExpansionHistory are included, are they carried in a SignedAttributes or AuthAttributes type, and not carried in a UnsignedAttributes, UnauthAttributes or UnprotectedAttributes type? [RFC 2634 1.3.4]		
If the attributes msgSigDigest, receiptRequest and signingCertificate are included, are they carried in a SignedAttributes type, and not carried in a AuthAttributes, UnsignedAttributes, UnauthAttributes or UnprotectedAttributes type? [RFC 2634 1.3.4]		
Does signerInfo not include multiple instances of any of the following attribute types: contentHints, contentIdentifier, eSSecurityLabel, msgSigDigest, mlExpansionHistory, receiptRequest, contentReference, equivalentLabels or signingCertificate? [RFC 2634 1.3.4,]		
If the attribute type contentHints, contentIdentifier, eSSecurityLabel, msgSigDigest, mlExpansionHistory, receiptRequest, contentReference, equivalentLabels or signingCertificate is present in a signerInfo, is there a single instance of AttributeValue? [RFC 2634 1.3.4]		
Are there zero or multiple, instances of AttributeValue present in the attrValues SET OF AttributeValue? [RFC 2634 1.3.4]		
If a counterSignature attribute is present, is it be included in the unsigned attributes and not included in the signed attributes? [RFC 2634 1.3.4]		
If a gateway or other processor adds a signerInfo to an existing signedData block, does it copy the mlExpansionHistory and eSSSecurityLabel attributes from other signerInfos? [RFC 2634 1.4]		
Is the recipient of the receipt the originator or a recipient of the original message? [RFC 2634 1.4]		
Is a ReceiptRequest attribute included in the attributes of a SignerInfo in a SignedData object that encapsulates a Receipt content? In other words, does the receiving agent request a signed receipt for a signed receipt? (No) [RFC 2634 2.2]		
Does the message originator populate the receiptsTo field with a GeneralNames for each entity to whom the recipient should send the signed receipt? [RFC 2634 2.2-4]		

REQUIREMENT FROM STANDARDS [1]	MET (Y/N/ na)	NOTES
Does the message originator include a GeneralNames for itself in the receiptsTo field when the originator wants the recipient to send the signed receipt to the originator? [RFC 2634 2.2-4]		
Does the message originator populate each entity's GeneralNames with the address to which the signed receipt should be sent? [RFC 2634 2.2-4]		
Do all of the SignerInfos that contain receipt requests have identical receipt requests? [RFC 2634 2.2.1]		
Does the sending agent retain one or both of the following items to support the validation of signed receipts returned by the recipients: a) The original signedData object requesting the signed receipt, or b) The message signature digest value used to generate the original signedData signerInfo signature value and the digest value of the Receipt content containing values included in the original signedData object? [RFC 2634 2.2.2]		
Does the receiving agent verify the signature of the SignerInfo which covers the receiptRequest attribute before processing a receiptRequest signedAttribute? (A recipient MUST NOT process a receiptRequest attribute that has not been verified.) [RFC 2634 2.3, 6]		
Does the processing software return any signed receipt if there are ReceiptRequest attributes which are not the same? (No) [RFC 2634 2.3]		
If a receiptRequest attribute is absent from the signed attributes, does the message recipient created a signed receipt? (No) [RFC 2634 2.3]		
If the mlReceiptPolicy value is none, is a signed receipt created? (No) (NOTE: The receipt policy of the Mail List supersedes the originator's request for a signed receipt.) [RFC 2634 2.3 (1.2.1)]		
If an mlExpansionHistory attribute is present, is a signed receipt created? (No) [RFC 2634 2.3 (2.2.1)]		
If receiptList does not contain one of the GeneralNames of the recipient, is signed receipt created? (No) [RFC 2634 2.3 (3.2)]		
Is the signature of the original signedData signerInfo that includes the receiptRequest signed attribute successfully verified before creating the signedData/Receipt? [RFC 2634 2.4 (1)]		

REQUIREMENT FROM STANDARDS [1]	MET (Y/N/ na)	NOTES
If the digest values of a signedData object are different (i.e., signature verification process fails) is a signedData/Receipt created? (No) [RFC 2634 2.4 (1.1)]		
If the signature verification fails, is a signedData/Receipt created? (No) [RFC 2634 2.4 (1.2)]		
Is a contentType attribute, including the id-ct-receipt object identifier, created and added to the signed attributes of the signerInfo (which will eventually contain the signedData/Receipt signature value)? [RFC 2634 2.4 (6)]		

Is the ASN.1 DER encoded Receipt content directly encoded within the signedData encapContentInfo eContent OCTET STRING? The format of the signedData encapContentInfo eContent OCTET STRING is as follows:
 	
SignedData ::= SEQUENCE {
version CMSVersion,
digestAlgorithms DigestAlgorithmIdentifiers,
encapContentInfo EncapsulatedContentInfo,
certificates [0] IMPLICIT CertificateSet OPTIONAL,
crls [1] IMPLICIT CertificateRevocationLists OPTIONAL,
signerInfos SignerInfos }, where
 	
EncapsulatedContentInfo ::= SEQUENCE {
eContentType ContentType,
eContent [0] EXPLICIT OCTET STRING OPTIONAL }
 	
[RFC 2634 2.4 (9) RFC 2630-5.1,5.2]		

Is the id-ct-receipt object identifier included in the signedData encapContentInfo eContentType? (This results in a single ASN.1 encoded object composed of a signedData including the Receipt content. The Data content type MUST NOT be used.) [RFC 2634 2.4 –(9)]		
Is the Receipt content encapsulated in a MIME header or any other header prior to being encoded as part of the signedData object? (No) [RFC 2634 2.4 (9)]		
If the signedData/Receipt is to be encrypted within an envelopedData object, then is an outer signedData object created that encapsulates the envelopedData object, and is a contentHints attribute with contentType set to the id-ct-receipt object identifier included in the outer signedData SignerInfo signedAttributes? [RFC 2634 2.4 (11)]		

REQUIREMENT FROM STANDARDS [1]	MET (Y/N/ na)	NOTES
If a sending agent supports the generation of ESS signed receipts, does it provide the ability to send encrypted signed receipts (that is, a signedData/Receipt encapsulated within an envelopedData)? [RFC 2634 2.4]		
Is an MLExpansionHistory attribute included in the attributes of a SignerInfo in a SignedData object that encapsulates a Receipt content? (No) [RFC 2634 2.4.1]		
If a signed receipt was created, then does the software use the following process to determine to whom the signed receipt should be sent? 1. The receiptsTo field must be present in the receiptRequest attribute. The software initiates the sequence of recipients with the value(s) of receiptsTo. 2. If the MlExpansionHistory attribute is present in the outer SignedData block, and the last MLData contains an MLReceiptPolicy value of insteadOf, then the software replaces the sequence of recipients with the value(s) of insteadOf. 3. If the MlExpansionHistory attribute is present in the outer SignedData block and the last MLData contains an MLReceiptPolicy value of inAdditionTo, then the software adds the value(s) of inAdditionTo to the sequence of recipients. [RFC 2634 2.5]		
In the process of validating a signedData/Receipt, is the message signature digest value calculated by the sender to generate the signature value included in the original signedData signerInfo that requested the signedData/Receipt acquired as follows? 3.1. If the sender-calculated message signature digest value has been saved locally by the sender, it is located and retrieved. 3.2. If it has not been saved, then it is re-calculated based on the original signedData content and signedAttributes. [RFC 2634 2.6-3, RFC 2630].		

REQUIREMENT FROM STANDARDS [1]	MET (Y/N/ na)	NOTES
In the process of validating a signedData/Receipt, is the digest value calculated by the sender for the Receipt content constructed by the sender (including the contentType, signedContentIdentifier, and signature value that were included in the original signedData signerInfo that requested the signedData/Receipt) acquired as follows? 5.1. If the sender-calculated Receipt content digest value has been saved locally by the sender, it is located and retrieved. 5.2. If it has not been saved, then it is re-calculated. [RFC 2634 2.6-5, RFC 2630].		
Is a signedContentIdentifier created by the message originator when creating a receipt request? [RFC 2634 2.7]		
Does the message originator populate the receiptsTo field with a GeneralNames for each entity to whom the recipient should send the signed receipt? [RFC 2634 2.7]		
Does the originator include a GeneralNames for itself in the receiptsTo field if the message originator wants the recipient to send the signed receipt to the originator? [RFC 2634 2.7]		
Are receipts encapsulated within a SignedData message? [RFC 2634 2.8]		
When a signedData/Receipt is encrypted within an envelopedData object, is an outer signedData object created that encapsulates the envelopedData object and is a contentHints attribute with contentType set to the id-ct-receipt object identifier included in the outer signedData SignerInfo signedAttributes? [RFC 2634 2.9]		
Does the first SignedData include a contentIdentifier signed attribute? [RFC 2634 2.11]		
If the sending agent is using security labels, are the labels put in the security label attribute in the signedAttributes field of a SignerInfo block? [RFC 2634 3.1.1]		
Is the security label attribute included in the unsigned attributes? (No) [RFC 2634 3.1.1]		
Are integrity and authentication security services applied to the security label and , therefore, is the security label included as a signed attribute, if used? [RFC 2634 3.1.1]		

REQUIREMENT FROM STANDARDS [1]	MET (Y/N/ na)	NOTES
Does the SignerInfo block have more than one security label signed attribute? (No) [RFC 2634 3.1.1]		
If any of the SignerInfos included in a SignedData object include an eSSSecurityLabel attribute, then do all of the SignerInfos in that SignedData object include an eSSSecurityLabel attribute and are the values of each identical? [RFC 2634 3.1.1]		
Does the receiving agent verify the signature of the SignerInfo which covers the eSSSecurityLabel attribute before processing an eSSSecurityLabel signedAttribute? [RFC 2634 3.1.2]		
Does the recipient process an eSSSecurityLabel attribute that has not been verified? (No) [RFC 2634 3.1.2]		
Does the receiving agent process the eSSSecurityLabel attribute, if present, in each SignerInfo in the SignedData object for which it verifies the signature? [RFC 2634 3.1.2]		
Does the receiving agent warn the user if the eSSSecurityLabels in the signerInfos that it verifies are not all identical? [RFC 2634 3.1.2]		
Is the security-classification value accompanied by a security-policy-identifier value to define the rules for its use? [RFC 2634 3.3.2]		
Is the set of valid security-classification values hierarchical? (NOTE: These values do not necessarily need to be in ascending numerical order.) [RFC 2634 3.3.2]		
Does the receiving agent process an equivalentLabels attribute in a message if the agent does not trust the signer of that attribute to translate the original eSSSecurityLabel values to the security policy included in the equivalentLabels attribute? (No) [RFC 2634 3.4]		
If an ESSSecurityLabel is present in a signerInfo, do all signerInfos in the signedData contain an ESSSecurityLabel and are they all identical? [RFC 2634 3.4.1]		
If present, does the equivalentLabels attribute include one or more security labels that are believed by the signer to be semantically equivalent to the ESSSecurityLabel attribute included in the same signerInfo? [RFC 2634 3.4.1]		
In the set of ESSSecurityLabel and EquivalentLabels security labels, are all security-policy object identifiers unique? [RFC 2634 3.4.1]		

REQUIREMENT FROM STANDARDS [1]	MET (Y/N/ na)	NOTES
Does a receiving agent ensure that all security-policy OIDs are unique in the security label or labels included in the EquivalentLabels before using an EquivalentLabels attribute? [RFC 2634 3.4.1]		
Once the receiving agent selects the security label (within the EquivalentLabels) to be used for processing, then does the agent compare the security-policy OID of the selected EquivalentLabels security label with the ESSSecurityLabel security-policy OID to ensure that they are unique? [RFC 2634 3.4.1]		
Are equivalentLabels used to convey security labels that are semantically different from the ESSSecurityLabel included in the signerInfos in the signedData? (No) [RFC 2634 3.4.1]		
If an entity needs to apply a security label that is semantically different from the ESSSecurityLabel, does it include the sematically different security label in an outer signedData object that encapsulates the signedData object that includes the ESSSecurityLabel? [RFC 2634 3.4.1]		
If present, is the equivalentLabels attribute a signed attribute? [RFC 2634 3.4.1]		
Does signerInfo include multiple instances of the equivalentLabels attribute? (No) [RFC 2634 3.4.1]		
Does the equivalentLabels attribute only include a single instance of AttributeValue? [RFC 2634 3.4.1]		
Are there zero or multiple instances of AttributeValue present in the attrValues SET OF AttributeValue? (No) [RFC 2634 3.4.1]		
If the policy in the ESSSecurityLabel is understood by the receiving agent, does the agent process that label and ignore all EquivalentLabels? [RFC 2634 3.4.2]		
When processing an EquivalentLabels attribute, does the receiving agent validate the signature on the EquivalentLabels attribute? [RFC 2634 3.4.2]		
Does the receiving agent act on an equivalentLabels attribute for which the signature could not be validated? (No) [RFC 2634 3.4.2]		
Does the receiving agent act on an equivalentLabels attribute only if that attribute is signed by an entity trusted to translate the original eSSSecurityLabel values to the security policy included in the equivalentLabels attribute? [RFC 2634 3.4.2]		

REQUIREMENT FROM STANDARDS [1]	MET (Y/N/ na)	NOTES
Does the sending agent create recipient-specific data structures for each recipient of an encrypted message? [RFC 2634 4.0]		
Does the MLA add an MLData record containing the MLA's identification information, date and time of expansion, and optional receipt policy to the end of the mail list expansion history sequence? [RFC 2634 4.1]		
If the mlExpansionHistory attribute is absent, does the MLA add the attribute so that the current expansion becomes the first element of the sequence? [RFC 2634 4.1]		
If the mlExpansionHistory attribute is present, does the MLA add the current expansion information to the end of the existing MLExpansionHistory sequence? [RFC 2634 4.1]		
If an MLA creates a SignerInfo that includes an mlExpansionHistory attribute, then do all of the SignerInfos created by the MLA for that SignedData object include an mlExpansionHistory attribute, and are the value of each identical? [RFC 2634 4.1]		
Does the recipient verify the signature of the SignerInfo which covers the mlExpansionHistory attribute before processing the mlExpansionHistory, and not process the mlExpansionHistory attribute unless the signature over it has been verified? [RFC 2634 4.1]		
If a SignedData object has more than one SignerInfo that has an mlExpansionHistory attribute, does the recipient compare the mlExpansionHistory attributes in all the SignerInfos that it has verified, and not process the mlExpansionHistory attribute unless every verified mlExpansionHistory attribute in the SignedData block is identical? [RFC 2634 4.1]		
If the mlExpansionHistory attributes in the verified signerInfos are not all identical, does the receiving agent stop processing the message? [RFC 2634 4.1]		
If an MLA finds its own identification information, does the MLA discontinue expansion processing?6 [RFC 2634 4.1.1]		
Does the MLA parse all layers of the received message to determine if there are any signedData layers that include an eSSSecurityLabel signedAttribute? [RFC 2634 4.2]		

REQUIREMENT FROM STANDARDS [1]	MET (Y/N/ na)	NOTES
Does the MLA fully process each eSSSecurityLabel attribute found in the various signedData layers, including performing access control checks, before distributing the message to the ML members? [RFC 2634 4.2]		
Does the MLA verify the signature of the signerInfo including the eSSSecurityLabel attribute before using it? [RFC 2634 4.2]		
Does the MLA sign the message to be sent to the ML members in a new "outer" signedData layer? [RFC 2634 4.2]		
Does the MLA add or update an mlExpansionHistory attribute in the "outer" signedData that it creates to document MLA processing? [RFC 2634 4.2]		
Except for when the MLA explicitly replaces an attribute (such as signingTime or mlExpansionHistory) with a new value, if there was an "outer" signedData layer included in the original message received by the MLA, then does the MLA-created "outer" signedData layer include each signed attribute present in the original "outer" signedData layer? [RFC 2634 4.2]		
When an S/MIME message is received by the MLA, does the MLA first determine which received signedData layer, if any, is the "outer" signedData layer? [RFC 2634 4.2]		
To identify the received "outer" signedData layer, does the MLA verify the signature and fully process the signedAttributes in each of the outer signedData layers (working from the outside in) to determine if any of them either include an mlExpansionHistory attribute or encapsulate an envelopedData object? [RFC 2634 4.2]		
If the MLA finds an "outer" signedData layer, then does the MLA perform the following steps: 1. Strip off all of the signedData layers that encapsulated the "outer" signedData layer 2. Strip off the "outer" signedData layer itself (after remembering the included signedAttributes) 3. Expand the envelopedData (if present) 4. Sign the message to be sent to the ML members in a new "outer" signedData layer that includes the signedAttributes (unless explicitly replaced) from the original, received "outer" signedData layer? [RFC 2634 4.2]		

REQUIREMENT FROM STANDARDS [1]	MET (Y/N/ na)	NOTES
If the MLA finds an "outer" signedData layer that includes an mlExpansionHistory attribute AND the MLA subsequently finds an envelopedData layer buried deeper with the layers of the received message, does the MLA strip off all of the signedData layers down to the envelopedData layer (including stripping off the original "outer" signedData layer) and sign the expanded envelopedData in a new "outer" signedData layer that includes the signedAttributes (unless explicitly replaced) from the original, received "outer" signedData layer? [RFC 2634 4.2]		
If the MLA does not find an "outer" signedData layer AND does not find an envelopedData layer, does the MLA sign the original, received message in a new "outer" signedData layer? [RFC 2634 4.2]		
If the MLA does not find an "outer" signedData AND does find an envelopedData layer does it expand the envelopedData layer, if present, and sign it in a new "outer" signedData layer? [RFC 2634 4.2]		
Unless the MLA explicitly replaces one or more particular attributes with new value, does the MLA create a signed attribute list for the new outermost signedData layer which includes each signed attribute present in the original outermost signedData layer? [RFC 2634 4.2.3.2 (3.2.3)]		
Does the MLA add an mlExpansionHistory signed attribute to the outer signedData layer as follows? 1. If the original outermost SignedData layer included an mlExpansionHistory attribute, the attribute's value is copied and updated with the current ML expansion information as described in the "Mail List Expansion" section. 2. If the original outermost SignedData layer did not include an mlExpansionHistory attribute, a new attribute value is created with the current ML expansion information as described in the "Mail List Expansion" section. [RFC 2634 4.2.3.2 (3.2.3)]		
Is the first certificate identified in the sequence of certificate identifiers the certificate used to verify the signature? [RFC 2634 5.4]		
If the hash of the certificate does not match the certificate used to verify the signature, is the signature considered invalid? [RFC 2634 5.4]		

REQUIREMENT FROM STANDARDS [1]	MET (Y/N/ na)	NOTES
If present, is the SigningCertificate attribute a signed attribute? [RFC 2634 5.4]		
Does a SignerInfo attribute include multiple instances of the SigningCertificate attribute? (No) [RFC 2634 5.4]		
Does a SigningCertificate attribute include only a single instance of AttributeValue? [RFC 2634 5.4]		
In the attrValues SET OF AttributeValue attribute, are there zero or multiple instances of AttributeValue present? (No) [RFC 2634 5.4]		
Is the issuer DN must be present in all signing certificates? [RFC 2634 5.4.1, RFC 2632]		
For non-attribute certificates, does the issuer contain only the issuer name from the certificate encoded in the directoryName choice of GeneralNames? [RFC 2634 5.4.1]		
For attribute certificates, does the issuer contain the issuer name field from the attribute certificate? [RFC 2634 5.4.1]		

Other information:

1. Requirement with a following (No) means that the answer to the question MUST be no.

Findings:

Recommendations for Standards Work: